ELSEVIER

Discrete Mathematics 132 (1994) 97–106

DISCRETE MATHEMATICS

Regulus codes☆

N.L. Johnson[a,*], Vikram Jha[b]

[a] *Department of Mathematics, The University of Iowa, 1A MLH, Iowa city, IA 52242, USA*
[b] *Department of Mathematics, Glasgow College, Glasgow G4 0BA, UK*

Received 23 June 1992

Abstract

In this article, the concept of partial spread code is introduced as a binary code with code words corresponding to the images of the partial spread under the associated projective semilinear group. The main result characterizes the regulus codes as a certain binary code.

1. Introduction

In [2], one of the authors developed a coding theoretic characterization of the Desarguesian line spreads within PG$(3,q)$ in terms of binary constant weight codes.

More generally in $\Sigma \cong \mathrm{PG}(2n-1,q)$, let σ be any $(n-1)$-dimensional spread. Order the $(n-1)$-dimensional subspaces $\Sigma=\{S_1,S_2,\ldots,S_N\}$ where

$$N=\prod_{k=1}^{n}(q^k+1)(q^{2k-1}-1)/(q^k-1).$$

Let F_2^N denote the space of N-tupes over GF(2) and for any collection of $(n-1)$-spaces γ in Σ, define $\bar{\gamma}=(x_1,x_2,\ldots,x_N)$ where $x_i=1$ iff $S_i\in\gamma$ and $x_i=0$ otherwise.

If σ is any spread then its code in F_2^N is defined as $C_\sigma=\{\overline{g(\sigma)}\mid g\in P\Gamma L(2n,q)\}$, and any binary code isomorphic to C_σ is called a *spread code*.

Theorem 1.1 (Jha [2, Theorem A]). *Let Ω be a constant weight binary code of type $(\omega=q^2+1,\ N=(q^2+1)(q^2+q+1))$, consisting of $1/2q^4(q^3-1)(q-1)$ code words. If $G\cong \mathrm{PSL}(4,q)$ is a transitive automorphism group of Ω then Ω is the code formed with codewords the Desarguesian line spread within* PG$(3,q)$. *Furthermore, G acts transitively*

☆ Part of this article was written when the authors were visiting the University of Lecce during May and June 1990. The authors express their appreciation to Professor Mauro Biliotti for arranging the visit and to the University of Lecce for support during this period.

* Corresponding author.

SSDI 0012-365X(93)E0006-P

on the code words. Conversely, the code C_σ of every Desarguesian spread σ, and no other spread code, has the above properties.

Actually, the above definition of spread codes may easily be extended to *partial spread codes* even though there is not an Andre' type theorem for recognition of isomorphic partial spreads of the same cardinality (degree).

Essentially nothing is known from a coding theory point of view regarding the characterization of partial spreads by their collineation groups.

Every partial spread gives rise to a net of the same degree. More generally, one of the present authors ([3]) recently proved the following theorem.

Theorem 1.2 (Johnson [3]). *Let R denote a finite net of degree $q+1$ and order q^2 which admits a collineation group isomorphic to* $\mathrm{PSL}(4, q)_N$ *where N is a line of the associated 3-dimensional projective space on which* $\mathrm{PSL}(4, q)$ *acts canonically.*

Then R is a derivable net and conversely, every finite derivable net of degree $q+1$ and order q^2 admits such a collineation group.

Concerning partial spreads in $\mathrm{PG}(2n-1, q)$, the ones of particular interest are the *derivable partial spreads*. In this case, each partial spread contains exactly q^n+1 $(n-1)$-dimensional projective spaces, and, if $q=p^r$, there is a set of q^n+1 $(nr-1)$-dimensional subspaces over $\mathrm{GF}(p)$ which forms a disjoint cover of the partial spread.

Also of basic importance are the *regulus partial spreads* in $\mathrm{PG}(2n-1, q)$ which are partial spreads of $q+1$ $(n-1)$-dimensional projective subspaces which admit a disjoint cover by a set of $(q^n-1)/(q-1)$ lines of $\mathrm{PG}(2n-1, q)$.

To combine all of the preceeding ideas, we isolate on the regulus partial spreads which are also derivable partial spreads. This forces the consideration of regulus partial spreads in $\mathrm{PG}(3, q)$.

Definition 1.3. If σ is any partial spread in $\mathrm{PG}(2n-1, q)$ then its code in F_2^N is $C_\sigma=\{\overline{g(\sigma)} \mid g\in P\Gamma\mathrm{L}(2n, q)\}$, and any binary code isomorphic to C_σ is called a partial spread code.

If σ is a derivable partial spread then C_σ shall be called a derivable code.

If σ is a regulus partial spread then C_σ shall be called a regulus code.

Thus, in this article, we shall be concerned with derivable codes which are also regulus codes; regulus codes from regulus partial spreads within $\mathrm{PG}(3, q)$. Also, and, henceforth, when referring to regulus codes, we shall mean within the context of $\mathrm{PG}(3, q)$.

We recall some basic combinatorics on reguli within $\mathrm{PG}(3, q)$.

Proposition 1.4. (i) *The number of reguli in a projective space* $\mathrm{PG}(3, q)$ *is* $q^4(q^3-1)(q^2+1)$.

(ii) $\mathrm{PSL}(4,q)$ *acts transitively on the reguli in* $\mathrm{PG}(3,q)$. *Thus, the stabilizer of a regulus within* $\mathrm{PSL}(4,q)$ *has order* $(q(q^2-1))^2/(4,q-1)$.

(iii) *Considering a regulus as a translation net within the associated 4-dimensional vector space* V_4 *over* $\mathrm{GF}(q)$, *then* $\mathrm{SL}(4,q)$ *acts transitively on the regulus nets and the stabilizer within* $\mathrm{SL}(4,q)$ *has order* $(q(q^2-1))^2$.

Since $\mathrm{PSL}(4,q)$ acts on $\mathrm{PG}(3,q)$ if and only if $\mathrm{SL}(4,q)$ acts on V_4, we may use either situation to study regulus codes. Normally, we shall work within V_4.

Proof. For (i) see [4, 48.3, p. 247].

(ii) Working in V_4, clearly the reguli are in an orbit under $\mathrm{GL}(4,q)$. The stabilizer of a regulus is a central product of two copies of $\mathrm{GL}(2,q)$ whose intersection is the center of either group. Let R and D be regulus nets in V_4. Also assume $g \in \mathrm{GL}(4,q)$ is such that $Rg=D$. Since within $\mathrm{GL}(2,q)$ there exist elements of all determinants, there is an element h within the stabilizer of D such that gh has determinant 1. Hence, there is an element of $\mathrm{SL}(4,q)$ which maps R onto D. □

Proposition 1.5. *A regulus code arising from the reguli in* $\mathrm{PG}(2,q)$ *is a binary constant weight* $\omega=q+1$ *code of length* $N=(q^2+1)(q^2+q+1)$, *which consists of* $q^4(q^3-1)(q^2+1)$ *code words and has minimum distance* $(q-1)$.

Proof. Except for the minimum distance, Proposition 1.5 follows from Proposition 1.4. Since two distinct reguli of $q+1$ lines can share at most two lines and there are pairs of reguli which do share two lines, the minimum distance is $q+1-2=q-1$. □

Our main result from the coding theoretic point of view is show the converse of Proposition 1.5.

Theorem 1.6. *Let* Ω *be a constant weight binary code of type* $(\omega=q+1, N=(q^2+1)(q^2+q+1))$, *with* $q^4(q^3-1)(q^2+1)$ *code words where* $q \neq 3$.

If $G \cong \mathrm{PSL}(4,q)$ *acts as a transitive automorphism group of* Ω *then* Ω *is isomorphic to the regulus code. Furthermore, the regulus code and no other partial spread code of* $\mathrm{PG}(3,q)$ *has the above properties.*

Considering the geometric aspect of the problem under consideration, we obtain the following result concerning the stabilizer of a set of $q+1$ lines within $\mathrm{PG}(3,q)$.

Theorem 1.7. *Let* R *be a set of* $q+1$ *lines within* $\mathrm{PG}(3,q)$ *which is left invariant by a subgroup* G *of* $\mathrm{PGL}(4,q)$ *of order divisible by* $(q(q^2-1))^2/(4,q-1)$ *where* $q \neq 3$. *Then* R *is a regulus and the group contains a subgroup isomorphic to* $\mathrm{PSL}(2,q) \times \mathrm{PSL}(2,q) \cong \mathrm{P}\Omega^+(4,q)$.

2. Reguli characterized by the order of a stabilizer subgroup

In this section, we prove Theorem 1.7 stated in the introduction. One approach to this problem would be to determine the possible subgroups of PGL(4, q) whose orders are divisible by $(q(q^2-1))^2/(4,q-1)$ with the intention to obtain a subgroup isomorphic to PSL(2, q) × PSL(2, q) and then show that if such a group leaves $q+1$ lines invariant then the lines must form a regulus. While this seems a reasonable approach, the group theory necessary takes us away from the combinatorial aspects of this study which we would like to emphasize. Thus, we give a combinatorial proof based simply on the group action of Sylow subgroups of various orders acting on a set of lines of cardinality $q+1$ within PG(3, q).

Thus, in this section, we assume that R is a set of $q+1$ lines with PG(3, q) which admits a collineation group within PG(3, q) of order divisible by $(q(q^2-1))^2/(4,q-1)$.

We shall prove Theorem 1.7 by a series of lemmas.

Lemma 2.1. *Considering the set within V_4, R is a set of $(q+1)$ 2-dimensional subspaces of V_4 admitting a collineation group G of order divisible by $(q(q^2-1))^2(q-1)/(4,q-1)$.*

We shall use the notation R_4 when considering the set R as a set of subspaces within V_4.

Proof. Take the preimage within GL(4, q) of any subgroup of PGL(4, q). The order of the preimage is $(q-1)$ times the order of the group. □

Lemma 2.2. *Let $L \in R_4$ and assume that t is the orbit length of L under G. Let $t = 2^b \cdot n \cdot s$ where s is odd and divides $(q+1)^2$ and n is odd and $(n,(q+1)^2)=1$. Then, $(q+1)^2/s$ is not divisible by $\bar{s}(q+1)$ where $\bar{s}$ is odd and >1.*

Notation 2.3. If k is any integer, we shall use the notation k_2 to denote the highest power of 2 which divides k and $k_{2'}$, to denote k/k_2 (the odd part of k).

Proof of Lemma 2.2. Suppose the lemma is false. Then $\bar{s} \mid (q+1)/s$. Let $G_{[L]}$ denote the subgroup of the stabilizer of L *which* fixes L pointwise.

First assume that $(\bar{s}(q+1)_{2'} \mid G_{[L]}\mid)=1$.

Hence, in $G_L \mid L$, there exists a subgroup of GL(2, q) of order divisible by $(\bar{s}(q+1))_{2'})$. However, $\mid \mathrm{GL}(2,q)\mid = q(q^2-1)(q-1)$ and $(q(q^2-1)(q-1),(\bar{s}(q+1))_{2'})=(q+1)_{2'}$. If $\bar{s} \mid (q+1)^2$, $\bar{s}$ odd and >1, we have a contradiction.

Thus, suppose $(\bar{s}(q+1)_{2'} \mid G_{[L]}\mid)>1$. Then there is an element $\tau \in G_{[L]}$ of odd order dividing $(q+1)^2$ and permuting the remaining q elements of R_4. Also since $((q+1)_{2'}(q-1)_{2'})=1$, it follows that τ fixes at least three elements of R_4.

Assume some two say N, M of the τ-fixed elements (lines of R) are not disjoint. Then τ must fix $N \cap M$ and leave invariant a set of $(q)1$-dimensional subspaces on each of N and M considering N and M as 2-dimensional vector subspaces. Without loss of generality, we may assume that the order of τ is a prime power >1 dividing $(q+1)$ and

hence, τ must fix each of the invariant 1-dimensional subspaces pointwise (as there are $q-1$ nonzero vectors on each such subspace) and hence τ must fix $N+M$ pointwise.

Since this forces τ to be a transvection in the associated projective space PG$(3,q)$, it follows $|\tau|\,|p(q-1)$ where $q=p^r$ which is a contradiction.

Thus, the three 2-dimensional subspaces of R_4 fixed by τ must be mutually disjoint. However, in this case, τ could not fix one of the 2-spaces pointwise because choosing a basis for the three 2-spaces appropriately, τ must have the form

$$\begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix}$$

and if one of the 2-spaces is fixed pointwise then $A=I$ so that $\tau=1$.

Hence, $\bar{s}(q+1)_{2'}$ cannot divide $(q+1)_{2'}^2$. This proves Lemma 2.2. □

Lemma 2.4. *For any $L\in R_4$, the length of the orbit of L is divisible by $(q+1)_{2'}$.*

Proof. The argument of Lemma 2.2 actually shows that if $p_j^{\beta_j}$ is the largest odd prime power of the prime p_j dividing $(q+1)$ then if $p_j^{e_j}$ divides $(q+1)^2/s$ then $e_j\leqslant\beta_j$. This, in turn, states that if $p_j^{\delta_j}$ is the largest prime power of p_j dividing s then $2\beta_j-\delta_j\leqslant\beta_j$ for all odd primes p_j dividing $(q+1)$. This implies that $(q+1)_{2'}$ must divided s and hence divides t which is the length of the orbit of L.

Lemma 2.5. *If q is even then the group acts transitively on the lines of* R. *If q is odd then each orbit is of length at least $(q+1)/2$.*

Proof. If q is even or q is odd but 4 does not divide $(q+1)$ then Lemma 2.5 follows from Lemma 2.4.

Thus, assume that $4|(q+1)$.

Let S be a Sylow 2-subgroup of G_L. Let the orbit length of L be t and let $t_2=2^b$ and $(q+1)_2=2^a$. Then $|S|$ is at least 2^{2a+2-b}. Since there are q(odd) remaining elements of R_4, S must fix one of the remaining elements. This leaves $(q-1)$ remaining elements and since $(q-1)_2=2$ under the assumption $4|q+1$, there must be at least one of these elements in an orbit under S of length 1 or 2. Thus, there is a 2-subgroup $\bar{S}$ of order at least 2^{2a+1-b} which fixes a third element. Suppose some pair of these 2-dimensional subspaces are not disjoint. Then $\bar{S}$ fixes the 1-subspace of intersection and since $(q-1)_2=2$, there is a subgroup S_1 of $\bar{S}$ of index at most 2 which fixes this subspace pointwise. Then S_1 fixes a 1-space of the remaining 1-spaces on the first invariant 2-subspace. Hence, there is a subgroup S_2 of S_1 of index at most 2 which fixes this second 1-space pointwise and similarly there is a subgroup S_3 of S_2 of index at most 2 which fixes the sum of the two 2-subspaces pointwise. Since the index of each of the subgroups listed in the previous subgroup listed is 1 or 2 in each corresponding containing group, it follows that $|S_3|$ is at least 2^{2a-b-2}. Since S_3 is a transvection

group, it follows that the elements of S_3 may be represented in the form

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ a & b & c & d \end{bmatrix}$$

for a, b, c, d in GF(q). Consider any such element $\tau \in S_3$. Then $\tau^{(q-1)}$ must have order divisible by p for $q = p^r$ so p is odd. Since $(q-1)_2 = 2$ and p is odd, it follows that $\tau^2 = 1$ and by the form of τ this implies that

$$\tau = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & d & e & \pm 1 \end{bmatrix} \quad \text{and} \quad c = d = e = 0 \text{ if } \pm = +.$$

If there exist elements $\neq 1 \tau_1, \tau_2$ then $\tau_1 \tau_2$ has order divisible by p so that $\tau_1 \tau_2 = 1$. Hence, $|S_3| \leqslant 2$ which implies that $2^{2a-b-2} \leqslant 2$ or rather that $2a-b-2 \leqslant 1$ so that $2a-3 \leqslant b$. By Lemma 2.4, $(q+1)_{2'} | t$ (for all such orbit lengths). If, for some L, also $b \geqslant 2a-3$, we would have $2^{2a-3}(q+1)_{2'} | 2^b (q+1)_{2'}$ which, in turn, divides t. However, $2^{2a-3} = (q+1)_2^2/8$ so that $(q+1)_2 (q+1)_2 (q+1)_{2'}/8$ (which is equal to $(q+1)_2 (q+1)/8$) must divide t which is $\leqslant q+1$. Hence, we have a contradiction unless possibly $(q+1)_2 \leqslant 8$. In this case, we obtain the following possibilities:

(1) $(q+1)_2 = 4$ and $t = (q+1)$ or $(q+1)/2$ or

(2) $(q+1)_2 = 8$ and $t = (q+1)$.

Hence, if $(q+1)_2 \leqslant 8$, we still have the proof to lemma provided that two of the three lines fixed by $\bar{S}$ are not disjoint.

So, in general, assume that the three 2-subspaces fixed by $\bar{S}$ are mutually disjoint. Recall that $|\bar{S}| \geqslant 2^{2a-b+1}$. It easily follows that $\bar{S}$ induces a faithful group in GL(2, q) so that $|\bar{S}| \,|(q(q^2-1)(q-1))_2 = 2^{a+2}$ (since $(q-1)_2 = 2$). Hence, $2a-b+1 \leqslant a+2$ or rather that $a-1 \leqslant b$. Using Lemma 2.4 again, we have $(q+1)_{2'} (q+1)_2/2$ must divide t. Hence, in this case, $(q+1)/2$ divides t. Thus we have the proof to Lemma 2.5.

We also point out the following consequence of our arguments.

Lemma 2.6. *If $(q+1)_2 > 8$ then for each 2-subspace $L \in R_4$, there are at least two other 2-subspaces in R_4 which are disjoint from L.*

Lemma 2.7. *If $(q+1)_2 \leqslant 4$ or 8 then either $q = 3$ or 7 or for every 2-subspace $L \in R_4$, there are at least two other 2-subspaces in R_4 which are disjoint from L.*

Proof. By Lemma 2.5, we know that $|G_L|$ is divisible by $e((q(q^2-1))^2(q-1))/((4, q-1)(q+1))$ for $e = 1$ or 2. Hence, $(q+1)$ divides the order of G_L. The argument within Lemma 2.2 shows that if $(q+1)_{2'} \neq 1$, then any element of odd order $\neq 1$ dividing

$(q+1)_{2'}$ must fix two other lines of R and the three lines are mutually disjoint. This proves the lemma. If $(q+1)_{2'}=1$ and $(q+1)_2 \leqslant 8$ then $q=3$ or 7. □

Lemma 2.8. *Assume $q \neq 3$ or 7. If G acts transitively then, for each element L of R_4, G_L contains a faithful p element for $p^r=q$. If G has two orbits of length $(q+1)/2$ then for at least one of the orbits Γ, the groups G_L for all $L \in \Gamma$ contain faithful p-elements.*

Proof. Each Sylow p-subgroup fixes a component L. For $q \neq 3$ or 7, there are elements disjoint from L. These elements disjoint from L must be permuted by G_L and hence by any Sylow p-subgroup of order q^2 in G_L (since the orbit length is $(q+1)$ or $(q+1)/2$). Thus, for any element N disjoint from L, there is a p-group in G_L of order at least q which fixes N. Since N and L are disjoint, this p-group must fix a distinct 1-space on each. Thus, within this p-group, each nonidentity element must act faithfully on at least one of L or N. This proves the lemma. □

Lemma 2.9. *Assume that $q \neq 3, 7$. Whenever G_L contains a nontrivial p-element, G_L acts transitively on the 1-spaces of L.*

Proof. $|G_L|$ is divisible by $e\,q^2(q+1)(q-1)^2/(4, q-1)$ where $e=1$ or 2 depending on whether we have transitivity on the lines of R or not.

Furthermore, we are assuming that we have a faithful p-element. This p-element must fix exactly one 1-space.

We have seen in Lemma 2.2 that any nonidentity element of order divisible by $(q+1)_{2'}$ within G_L must act faithfully on L.

If $p=2$ (so that $e=1$), then the faithful part of G_L is divisible by $(q+1)$ and 2 so that clearly we must have transitivity on the 1-spaces of L.

Now assume that $(q+1) \neq 2^a$ and that q is odd. Then, there is a prime p-primitive divisor u of (q^2-1) and a faithful element in G_L of order u. Since, there are p-elements and p-primitive elements in G_L which act faithfully on L, it must be that the p-elements generate SL(2, 5) with $q=9$ or SL$(2, q)$ and, in either case, we have the required transitivity on the 1-spaces of L.

Now assume that $q+1=2^a$ for some integer a. Since $q \neq 3$ or 7, we may assume that $a \geqslant 5$. Recall again that the order of G_L is divisible by $e\,q^2(q+1)(q-1)^2/(4, q-1)$ where $e=1$ or 2. Hence, a Sylow 2-subgroup S of G_L has order at least $2(q+1)$.

Since $(q+1)_2 > 8$, by following the argument of Lemma 2.5, there is a 2-group $\bar{S}$ of order at least $(q+1)$ which fixes at least two other mutually disjoint 2-subspaces of R_4. Hence, $\bar{S}$ must act faithfully on L. Consider the quotient $G_L/G_L \cap$(Center of $G)|L \leqslant$ PGL$(2, q)$. Within this group must appear a $p-$element and a subgroup of order divisible by at least $(q+1)/2$. Taking the further intersection with PSL$(2, q)$, we obtain a subgroup of order divisible by p and by $(q+1)/4$. Since we know explicitly the subgroups of PSL$(2, q)$, suppose there is a normal p-group. Then $(q+1)/4|(q-1)_2=2$ so that $(q+1)=4$ or 8 contrary to our assumptions.

Hence, the group generated by the p-elements must be isomorphic to A_4, A_5, S_4, or contain a normal subgroup isomorphic to $\mathrm{PSL}(2, p^s)$ for $q = p^r$. If $q \neq 31$ then the first three cases cannot occur since the order of the 2-subgroup is at least $(q+1)/4 > 8$. However, $q \neq 31$ either because 31 does not divide the order of these special groups.

If we do not obtain transitivity in the case $\mathrm{PSL}(2, p^s)$ then $s|r$ (see e.g. [1, p. 213, (8.27)]) and so $p^s \leqslant q^{1/2}$.

Now the 2-group $\bar{S}$ acts faithfully on L and of order at least $(q+1)$. The stabilizer subgroup $\hat{S}$ within $\bar{S}$ of a 1-space within L can have order at most 4 by previous arguments ($\bar{S}$ must fix another 1-space on L since $(q-1)_2 = 2$ and a subgroup of $\hat{S}$ of order $\geqslant |\hat{S}|/4$ would fix L pointwise). Hence, each orbit length is at least $(q+1)/4$ and hence $q^{1/2} + 1 \geqslant p^s + 1 \geqslant (q+1)/4$ if and only if $22q - 9 \geqslant q^2$. The smallest value of $q \geqslant 31$ so that this cannot occur.

Hence, we have the required transitivity of G_L whenever $q \neq 3$ or 7 and there exist faithful p-elements.

Corollary 2.10. *If $q \neq 3, 7$ then for at least $(q+1)/2$ of the lines L or R, G_L acts transitively on the 1-subspaces of L.*

Lemma 2.11. *If $q \neq 3, 7$ then for each line L of R, G_L acts transitively on the 1-subspaces of L.*

Proof. If Lemma 2.11 is not valid then q is odd and there are two orbits of length $(q+1)/2$ denoted by Γ_1 and Γ_2. Assume that for $L \in \Gamma_1$, G_L acts transitively on the 1-subspaces of L. Also assume that for any $N \in \Gamma_2$, G_N does not act transitively on the 1-subspaces of N. By previous arguments, it follows that there is no faithful p-element in G_N. Now let S denote a Sylow p-subgroup of order at least q^2 in G_N. Hence, S fixes N pointwise. Also since there are $(q+1)/2$ lines of Γ_1, then S fixes at least two elements L, M of Γ_1. Now since G_L, G_M act transitively on the 1-subspaces of L, M, respectively, and since there are but $q+1$ lines of R, it follows that L, M, and N are mutually disjoint. However, no transvection can fix three disjoint lines.

Hence, each group G_Z for all $Z \in R_4$ acts transitively on the 1-subspaces of Z.

This proves Lemma 2.11. □

Note that since there are but $q+1$ elements of R_4, we obtain the following results.

Corollary 2.12. *If $q \neq 3, 7$ then R_4 is a partial spread; R is a set of disjoint lines.*

Theorem 2.13. *If $q \neq 3, 7$ then R is a regulus.*

Proof. Consider any element L of R_4. Then for any element $N \in R_4 - \{L\}$, there is a p-subgroup of G_L, S_N of order $\geqslant q$ which fixes both L and N and hence fixes a 1-dimensional subspace on each. Now since this leaves $q-1$ elements of R_4, S_N must fix another element M of R_4. However, since these three elements are mutually

disjoint, it follows that no element of S_N can be a transvection within PG$(3,q)$. Hence, S_N fixes exactly a 2-dimensional subspace pointwise and every nonidentity element fixes exactly this subspace pointwise.

Now consider the line L within PG$(3,q)$. Since there are exactly $q+1$ planes containing L, there is at least one, say π, which is left invariant by S_N. Since the $q+1$ lines of R are mutually disjoint (skew) none of these lines $\neq L$ can lie in π. Hence, each of the lines $\neq L$ intersect π in a point. S_N becomes an elation group in π with fixed line the join of the 1-spaces (as points) on L, N fixed pointwise by S_N. Since S_N has order $\geqslant q$, it follows that none of the remaining lines can lie off of the axis of S_N for this would force an orbit of at least q additional lines different from L and N (recall again that the lines are disjoint and each is moved if it does not lie on the axis of S_N).

Hence, the axis of S_N (fixed point subspace) intersects each of the $q+1$ lines of R and hence becomes a transversal to R. However, G_L acts transitively on the 1-spaces of L. Hence, here is another such group $\bar{S}_N$ fixing L which fixes a different 1-space of L than does S_N. Also, note that the group S_N, as an elation group of π, must have center on L since L is fixed. Hence, the order of S_N is exactly q as there are no transvections in S_N.

Thinking of L as a Desarguesian spread, the group generated by S_N and $\bar{S}_N$ on L must be either:

SL$(2,5)$ and $q=3$ or for $q>2$, SL$(2,q)$. Hence, we may assume that we obtain SL$(2,q)$ on L and this group acts faithfully on L since both S_N and $\bar{S}_N$ fix each of the $q+1$ lines of R.

Now assume that S_N and $\bar{S}_N$ fix the same point on N. Then SL$(2,q)$ fixes N and a 1-space on N. By the argument of Johnson ([3, 3.2]), SL$(2,q)$ either fixes N pointwise or $q=2,3,5,7,9$, or 11. However, this would force a transvection back in S which cannot be the case. Hence, each two groups S_N and $\bar{S}_N$ have disjoint fixed point spaces and the set of these fixed point spaces form the set of $q+1$ transversals to the lines of R. That is, R is a regulus.

However, for the special cases, $q=2,5,9$, or 11 (see e.g. [1, 8.28, p. 214]), if there is a fixed 1-space on N then there must be an element of p-primitive order fixing N pointwise. However, we have seen that this cannot be the case.

We now consider the cases $q=3,7$. First assume $q=7$.

In this case, there must be one orbit of length 8. Let L_1 be any line. Then, a Sylow 2-group of order 2^5 in G_{L_1} must fix another line L_2. The arguments of Lemma 2.5 show that L_1 and L_2 are disjoint.

Sine a Sylow 7-subgroup in G_{L_1} has order 7^2, there exists a subgroup which leaves both lines invariant and hence, there must be a faithful 7-element on one of these lines and by transitivity on the lines, there must be a faithful 7-element on any line.

Assume that G_{L_1} is not transitive on the 1-spaces of L_1. So, G_{L_2} is not transitive on the 1-spaces of L_2. Then the faithful part of G_{L_1} has order divisible by $7{\cdot}6{\cdot}6$ (by factoring our the possible center of GL$(2,7)$). Hence, there is a 2-group of order $\geqslant 2^3$ which fixes L_1 pointwise and, of course, leaves L_2 invariant. However, since the group G_{L_2} contains a faithful 7-element and the group is not transitive on the 1-spaces of L_2,

it must be that the 2-group of G_{L_1} which fixes L_1 pointwise, must leave invariant a 1-space of L_2. However, this would say that there is a 2-group of order $\geqslant 2^2$ which fixes a 3-space pointwise, which is a contradiction since $(7-1)_2=2$.

In this way, we see that we have a set of 8 mutually skew lines (a partial spread).

The 7-group which fixes L_1 and L_2 must fix the remaining 6-lines and fix a 2-space pointwise which must lie across each line. This is a transversal to the set of 8 lines.

Since we have transitivity on each line, we are finished unless possibly SL(2, 7) acting canonically on L_1 fixes a 1-space of L_2. However, as we may realize SL(2, 7) faithfully as a collineation group of L_2 as an affine Desarguesian plane of order 7 which leaves a line invariant, this clearly cannot occur.

Hence, the main result is valid for $q=7$. Now we assume $q=3$.

The main result is not valid for $q=3$. *For example, the set of lines could be a set of* 4 *lines of a plane* π_0 *of* PG(3, 3) *which are incident with a point* P *of* π_0.

The order of $GL(4,3)_{P,\pi_0}$ may be seen to have order divisible by $q^7(q+1)(q-1)^4$ by considering the subgroup of order $q^3(q-1)$ which fixes π_0 pointwise and then considering the stabilizer of a 1-space within GL(3, 3).

The group which we are considering has order divisible by $(q(q^2-1))^2(q-1)/(4,q-1)$. We see that this group can be a subgroup of $GL(4,3)_{P,\pi_0}$ provided $(q+1)/(4,q-1)$ divides $q-1$.

This occurs when $q+1=4$.

Continuing with the statement involving the type of group we actually have, if R is a regulus then within PSL(4, q) the stabilizer of R contains $PSL(2,q)\times PSL(2,q)$ and is of index 1 or 2 within the full stabilizer. Hence, we may assume that the group G in question and $PSL(2,q)\times PSL(2,q)$ both stabilize a regulus. That is, we may assume that there is a subgroup of the associated projective orthogonal group which contains both G and $PSL(2,q)\times PSL(2,q)$. Since the stabilizer of a regulus in PGL(4, q) is $PGL(2,q)\times PGL(2,q)$, it is easy to verify that G must then contain $PSL(2,q)\times PSL(2,q)\cong P\Omega^+(4,q)$.

3. Characterization of regulus codes

Assume the conditions of Theorem 1.6.

As observed in [2, p. 93], PSL(4, q) has a unique transitive representation on $N=(q^2+1)(q^2+q+1)$ letters as each subgroup with index N is congugate. Hence, we have the proof to Theorem 1.6 stated in the introduction.

References

[1] B. Huppert, Endliche Gruppen (Springer, Berlin, 1980).
[2] V. Jha, On binary constant weight codes associated with spreads, Ars Combin. 29 A(1990) 91–96.
[3] N.L. Johnson, A group theoretic characterization of finite derivable nets, J. Geom. 9 (1991) 105–112.
[4] H. Lüneburg. Translation Planes (Springer, Berlin, 1980).